

**COMUNE DI GENOVA**

**DIREZIONE TECNOLOGIE DIGITALIZZAZIONE E SMART CITY**

**SETTORE PROGRAMMAZIONE E REALIZZAZIONE**

**ACQUISIZIONE DI SERVIZI DI MANUTENZIONE EVOLUTIVA E ADEGUATIVA PER LA PIATTAFORMA DEI PAGAMENTI (MIP - MODULO INCASSI E PAGAMENTI E PUNTO UNICO DI EMISSIONE) DEL COMUNE DI GENOVA**

**ALLEGATO 20 – Specifiche integrazione POS**

**Sommario**

[1. Obiettivo 2](#_Toc114148690)

[2. Acronimi 3](#_Toc114148691)

[3. Scenario “Scambio Importo Remoto” 3](#_Toc114148692)

[3.1 POST …/remote/payments 3](#_Toc114148693)

[3.2. POST …/remote/payments/{id}/amount-exchange 5](#_Toc114148694)

[3.3. GET …/remote/payments/{id}/status 6](#_Toc114148695)

[4. Sicurezza 7](#_Toc114148696)

# 1. Obiettivo

Questo documento illustra le principali interfacce messe a disposizione dall’Ente per l’integrazione con i POS messi a disposizione dal Civico Tesoriere.

Le interfacce, esposte sull’Enterprise Service Bus dell’Ente (WSO2), si presentano come REST Application richiamabili tramite protocollo sicuro HTTPS (TLS 1.2) da un processo CLIENT previa autenticazione.

Le specifiche di sicurezza prevedono la comunicazione di un token di validazione prelevato tramite un’apposita chiamata e con durata limitata.

# 2. Acronimi

|  |  |
| --- | --- |
| **Acronimo** | **Definizione** |
| PA | Pubblica Amministrazione |
| DP | Data ProviderIdentifica l’organizzazione che, incaricata direttamente (come partner tecnologico) o indirettamente (come intermediario per conto della PA o del Partner Tecnologico incaricato) interagisce con il sistema di interfacciamento remoto attraverso un proprio processo/applicazione CLIENT di interrogazione |
| UTENTE | Utente finaleIdentifica il soggetto che esegue il pagamento |
| POS | Terminale POSIdentifica il terminale POS utilizzato per il pagamento |
| WWS | WEB Service (per l’attivazione remota del POS)Identifica il WEB Service Rest pubblicato e richiamabile via protocollo sicuro HTTPS dal processo CLIENT |

# 3. Interfacce per gestione dello scenario “Scambio Importo Remoto”

## 3.1 POST …/remote/payments

Questo endpoint inserisce il pagamento nel sistema per la verifica.

URL di esempio: *POST* https://<server\_name>:<server\_port>/Payment/remote/payments/

Il gestionale di cassa dell’Ente invia a WWS i seguenti dati di input:

* providerTrackId è ID dell’operazione generato dal sistema chiamante.
* Codice Associato all’ente presente SU BO
* terminalId è l’ID del terminale logico assegnato dal Gestore Terminali POS
* userid è il codice di avviso pagamento
* billerVatNumber è la Partita IVA dell’Ente
* toolType
* toolTypeVersion

La descrizione dettagliata dei campi verrà fornita tramite opportuno documento.

WWS restituisce:

 HTTP Status 201: se il risultato dell’operazione è "0000" e lo stato del bollettino è PAYABLE. Nel body della risposta sono presenti le informazioni del pagamento;

 HTTP Status 406: Se il risultato dell’operqazione non è "0000" o lo stato del bollettino non è PAYABLE;

 HTTP Status 401/403: Se la quantità di sicurezza x-jws-signature non è valida



|  |  |  |  |
| --- | --- | --- | --- |
|   |  |  |  |
| **Response:** ***Element***   | ***Description***   | ***M/O***   | ***Additional info***   |
| **result**   | Esito dell’operazione  | M  | 0000 = Operazione eseguita con successo Per qualsiasi altro codice siamo in presenza di un errore. In presenza di errori è valorizzato il campo errorMessage.  |
| **errorMessage**   | Descrizione dell’errore  | O  | Valorizzato solo in presenza di errori  |
| **id**   | ID operazione di WWS  | M\*  | È l’ID operazione restituito dalla componente server WWS. Viene sempre valorizzato anche in caso di errori  |
| **transactionID**   | ID transazione del pagamento restituito dal Sistema intermediario di SIA  | M\*  | È l’ID operazione restituito dalla componente server WWS. Viene sempre valorizzato anche in caso di errori  |
| **providerTrackId**   | Restituisce lo stesso valore recepito come parametro di ingresso dall’omonimo campo.  | M\*  |  |

**billData / Esempio** Dati del tributo M\* L’oggetto è in fase di "billData": { definizione

"userId":

"001921132000000132", "payerTaxCode":

"ZNRMSM71B08L219Z",

"billerId": "BDXFZ",

"billerName": "COMUNE DI ARZANO",

"billerTaxCode":

"80029290634",

"amount": 1.2,

"totalChargedFees": 0,

"totalAmount": 1.2, "currency": "EUR", "number":

"921132000000132",

"referencePeriod": "N/A", "status": "PAYABLE",

"channelTransactionId":

"00012513275",

"moreInfos": [

{

"name": "CAUSALE

VERSAMENTO",

"value": "CARTA DI

IDENTITÀ MOD.34560"

},

{

"name": "BENEFICIARIO",

"value": "COMUNE DI

ARZANO"

}

],

"pspData": {

"name": "Unicredit SPA",

"id": "ABI02008",

"taxCode": "00348170101"

},

"shopData": {

"name": "COMUNE DI

VERONA",

"address": "VIA VITTORIO

EMANUELE II",

"town": "VERONA"

},

}

}

## 3.2. POST …/remote/payments/{id}/amount-exchange

Questa interfaccia avvia il processo di pagamento con la chiamata di scambio importo remoto.

Il placeholder {id} indica l’identificativo univoco del pagamento (UUID) al’interno del sistema integratore WWS.

URL di esempio: POST https://<server\_name>:<server\_port>/Payment/remote/payments/{id}/amount-exchange

Il gestionale di cassa dell’Ente invia a WWS i seguenti dati di input:

* id è l’identificativo univoco del pagamento (UUID) al’interno del sistema integratore WWS. Questo dato è presente nel body della risposta dell’endpoint **POST /remote/payments**
* providerTrackId è ID dell’operazione generato dal sistema chiamante.
* transactionId è l’ID della transazione del Network (FastBank)
* terminalId è l’ID del terminale logico assegnato dal Gestore Terminali POS
* userid è il codice di avviso pagamento
* payerTaxCode è il Codice Fiscale del pagatore
* billerVatNumber è la Partita IVA dell’Ente
* toolType è un valore fisso da concordare
* toolTypeVersion è un valore fisso da concordare

WWS restituisce:

* HTTP Status 200: se la chiamata per lo scambio importo remoto è stata eseguita correttamente; 

 HTTP Status 406: o Se l’attributo “result” = “9919” e l’attributo “rateLimitReset” è impostato, si deve riprovare dopo la data e l'ora specificate nell'attributo “rateLimitReset”;

* + Se l’attributo “result” = “9919” e l’attributo “rateLimitReset” non è impostato, si deve riprovare senza indicazioni di data e ora;
	+ Se l’attributo “result” <> “9919”, deve restituire un messaggio di errore generico

|  |  |  |  |
| --- | --- | --- | --- |
|   |  |  |  |
| **Response:** ***Element***   | ***Description***   | ***M/O***   | ***Additional info***   |
| **result**   | Esito dell’operazione  | M  | 0000 = Operazione eseguita con successo Per qualsiasi altro codice siamo in presenza di un errore. In presenza di errori è valorizzato il campo errorMessage.  |
| **errorMessage**   | Descrizione dell’errore  | O  | Valorizzato solo in presenza di errori  |
| **id**   | ID operazione di WWS  | M\*  | È l’ID operazione restituito dalla componente server WWS. Viene sempre valorizzato anche in caso di errori  |
| **providerTrackId**   | Restituisce lo stesso valore recepito come parametro di ingresso dall’omonimo campo.  | M\*  |  |
| **rateLimitReset**     | Data in formato unix ora in cui una richiesta di notifica push   | O  |  |

## 3.3. GET …/remote/payments/{id}/status

Questa interfaccia consente di verificare lo stato del pagamento.

URL di esempio:

GET https://<server\_name>:<server\_port>/ /Payment/remote/payments/{id}/status

Il gestionale di cassa dell’Ente, invia a WWS i seguenti dati di input:

• {id} è l’identificativo univoco del pagamento (UUID) al’interno del sistema integratore WWS. Questo dato è presente nel body della risposta dell’endpoint **POST /remote/payments**

WWS restituisce:

 HTTP Status 200: se lo stato del pagamento è letto correttamente.

Tutti i possibili stati gestiti da WWS saranno descritti con apposito documento.

|  |  |  |  |
| --- | --- | --- | --- |
| **Response:** ***Element***   |  ***Description***   |  ***M/O***   |  ***Additional info***   |
| **result**   | Esito dell’operazione  | M  | 0000 = Operazione eseguita con successo Per qualsiasi altro codice siamo in presenza di un errore. In presenza di errori è valorizzato il campo errorMessage.  |
| **errorMessage**   | Descrizione dell’errore  | O  | Valorizzato solo in presenza di errori  |
| **status**     | Stato del Pagamento  | M\*  |  |
|   |   |  |  |

# 4. Sicurezza

Per utilizzare le API esposte da WSO2, è necessario utilizzare un token per farsi autenticare dalla piattaforma API Manager WSO2 (Access Token OAuth).

Il token di accesso oauth (chiamato per comodità Access Token OAuth) consente al chiamante di identificarsi sulla Piattaforma WSO2. Il token viene rilasciato sulla base di un processo di invocazione di una apposita interfaccia:

|  |
| --- |
| URL di esempio:  |

GET https://<server\_name>:<server\_port>/manageToken/getToken?Key=xxxxxx&Secret=zzzzzzzz

Dove xxxxx e zzzzz sono da sostituire con key e secret forniti in maniera apposita.

Risposta:

{

 "access\_token": "35b550e8-468b-30c0-b16c-4fc52990bd35",

 "scope": "am\_application\_scope default",

 "token\_type": "Bearer",

 "expires\_in": 3600

}

La risposta fornisce un access\_token con durata limitata indicata in "expires\_in” (in secondi).